RSAC 2025 Conference

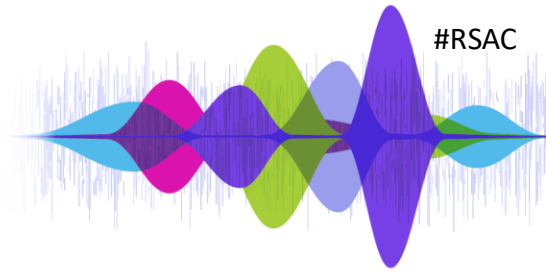
Many Voices.
One Community.

SESSION ID: CTF-T01

Advanced Exploit Writing, Hunting, and Defense CTF

Parker Garrison

Founder, Iguana Cyber
linkedin.com/in/parkergarrison



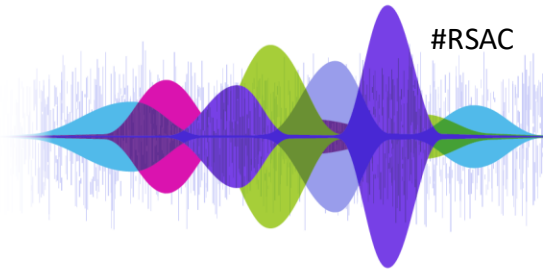
Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

The views and statements expressed by the speaker in this presentation are the same as the official views of Iguana Cyber, LLC.



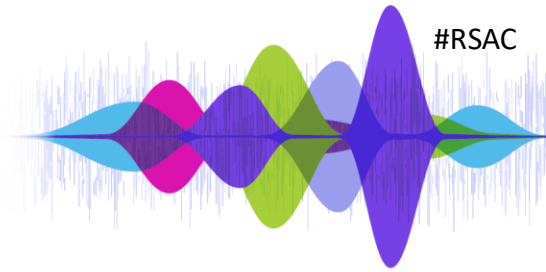
Objectives

- Use ElasticSearch to perform exploit hunting
- Rewrite the exploit (Threat Emulation) to use against your opponents and score points
- Secure the system against exploits using Consensus-Based Defense
- Test the security of your new system

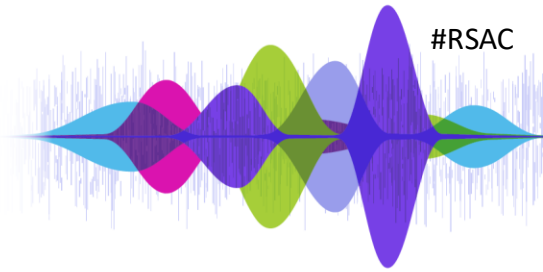
Connect to your instance

- Example: ssh student@[ip address]

And the winners are…



Live Solution Demonstration



- Step 1: Finding the Exploit
  - In ElasticSearch, search for instances where the HTTP response from the primary and secondary server mismatch
- Step 2: Rewriting the Exploit
- Step 3: Defense
  - Identify the IP addresses and the ports of the primary and secondary server
  - Restart the server

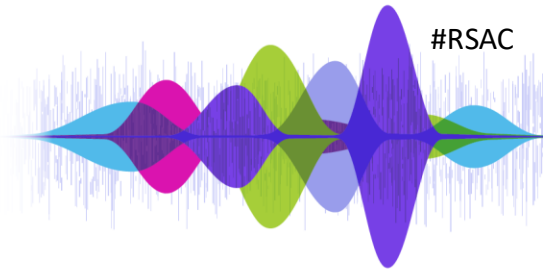
Summary

- In simple or complex programs, you can bypass state-of-the-art exploit mitigations including ASLR, DEP/NX, and Stack Cookies (as you just did!)
- Layering exploit mitigations makes an attacker's job a bit harder, but:
- **Consensus-Based Defense makes an attacker's job exponentially harder** as they require one attack to work simultaneously and identically on: 2 different memory layouts, OSes, processors, and exploit mitigations

Apply

- Within 1 week:
  - Identify which webservers can access private or critical information or systems
- Within 1 month:
  - Identify & Test a Consensus-Based Defense solution for each of these webservers
- Within 2 months:
  - Deploy the Consensus-Based Defense solution in Permissive mode, and see if there are any unintentional mismatches
- Within 3 months:
  - Set the Consensus-Based Defense solution into Enforcing mode
- Within 6 months:
  - Identify and test alternate runtime and compile-time exploit mitigations for use on two or more of the backend servers
  - Implement those exploit mitigations
- Within one year:
  - Update processes in use for webserver deployment to include a Consensus-Based Defense solution from the start

Further Reading and Practice



- Consensus Based Defense: youtu.be/YAGmZv11xvU *
- Exploit Development:
  - A “Crash” Course in Buffer Overflows: youtu.be/0xlqpB07GHo *
  - Gray Hat Hacking, 6th Edition, by Stephen Sims et. al *
  - Modern Binary Exploitation: https://github.com/RPISEC/MBE

* Also by this presenter

* Available in Conference Bookstore while supplies last

RSAC™ | 2025 Conference

Many Voices.
One Community.